

1 CLAIMS:

3 1. A computer-readable medium having computer-executable
4 instructions that, when executed by a computer, performs a method comprising:

5 obtaining a message M having two portions, wherein M_1 is one of the
6 portions of the M and M_2 is another;

7 generating one or more codes having a combination with M_2 implicitly
8 embedded therein, wherein calculations that generate the one or more codes do not
9 employ M_2 ;

10 reporting the one or more codes.

11
12 2. A medium as recited in claim 1, wherein the method further
13 comprises producing a digital signature (DS) comprising M_1 and the reported one
14 or more codes.

15
16 3. A medium as recited in claim 1, wherein two or more codes are
17 generated by the generating and reported by the reporting.

18
19 4. A medium as recited in claim 3, wherein a mathematical function for
20 calculating one code is not identical to a mathematical function for calculating
21 another code.

1 5. A medium as recited in claim 3, wherein the message M has a
2 defined length and a length of a combination of two or more codes is less than the
3 message's defined length.

4

5 6. A medium as recited in claim 3, wherein M_2 has a defined length and
6 a length of a combination of two or more codes is less than or equal to the defined
7 length of M_2 .

8

9 7. A medium as recited in claim 1, wherein the generating comprises:
10 finding a value of a variable per-message key (k) where a predefined
11 mathematical function employing k produces a result equivalent to M_2 ;
12 when such a value of k is found, calculating the two or more codes, where
13 the calculation of one code is not identical to the calculation of any other code and
14 where each calculation incorporates k .

15

16 8. A medium as recited in claim 1, wherein the generating comprises:
17 finding a value of a variable per-message key (k) where a predefined
18 mathematical function employing k produces a result equivalent to M_2 ;
19 when such a value of k is found, calculating the two or more codes, where
20 the calculation of one code is not identical to the calculation of any other code, the
21 calculation of at least one code employs non-linear mathematical function, namely
22 a quadratic equation, and where each calculation incorporates k .

1 **9.** A medium as recited in claim 3, wherein the generating comprises:
2 finding a value of a variable per-message key (k) where a predefined
3 mathematical function employing M_1 and g^k produces a result equivalent to M_2 ;
4 when such a value of k is found, calculating the two or more codes, where
5 one code is r and another is s , with r being calculated using another predefined
6 mathematical function employing M_1 and g^k , and with s being calculated using still
7 another predefined mathematical function employing M_1 and g^k and r .

8

9 **10.** A medium as recited in claim 3, wherein the method further
10 comprises producing a digital signature (DS) comprising M_1 and the reported codes
11 r and s .

12

13 **11.** A computing device comprising:
14 an audio/visual output;
15 a medium as recited in claim 1.

16

17

18

19

20

21

22

23

24

25

1 **12.** A computer-readable medium having computer-executable
2 instructions that, when executed by a computer, performs a method comprising:

3 obtaining a message M having two portions, wherein M_1 is one of the
4 portions of the M and M_2 is another;

5 generating two or more codes having a combination with M_2 implicitly
6 embedded therein, wherein calculations that generate the codes do not employ M_2 ,
7 wherein the generating comprises:

- 8 • finding a value of a variable per-message key (k) where a predefined
9 mathematical function employing M_1 and g^k produces a result
10 equivalent to M_2 ;
- 11 • when such a value of k is found, calculating the two or more codes,
12 where the calculation of one code is not identical to the calculation
13 of any other code and where each calculation incorporates k ;

14 reporting the two or more codes.

15
16 **13.** A medium as recited in claim 12, wherein the method further
17 comprises producing a digital signature (DS) comprising M_1 and the reported two
18 or more codes.

19
20 **14.** A medium as recited in claim 12, wherein the calculation of at least
21 one code employs a non-linear mathematical function.

1 **15.** A medium as recited in claim 12, wherein the message M has a
2 defined length and a length of a combination of two or more codes is less than the
3 message's defined length.

4

5 **16.** A medium as recited in claim 12, wherein M_2 has a defined length
6 and a length of a combination of two or more codes is less than or equal to the
7 defined length of M_2 .

8

9 **17.** A medium as recited in claim 12, wherein one calculated code is r
10 and another is s , with r being calculated using another predefined mathematical
11 function employing M_1 and g^k , and with s being calculated using still another
12 predefined mathematical function employing M_1 and g^k and r .

13

14 **18.** A medium as recited in claim 17, wherein the predefined
15 mathematical function for s is non-linear.

16

17 **19.** A medium as recited in claim 17, wherein the method further
18 comprises producing a digital signature (DS) comprising M_1 and the reported codes
19 r and s .

20

21 **20.** A computing device comprising:
22 an audio/visual output;
23 a medium as recited in claim 12.

1 **21.** A computer-readable medium having computer-executable
2 instructions that, when executed by a computer, performs a method comprising:

3 obtaining a digital signature (*DS*) having at least three portions, M_1 , r , and
4 s ;

5 using a first predefined mathematical function employing M_1 , r , and s ,
6 calculating the value of gk ;

7 determining whether a second predefined mathematical function employing
8 M_1 and gk produces a value equivalent to r

9 indicating the result of such determining.

10
11 **22.** A medium as recited in claim 21, wherein the method further
12 comprises:

13 using a third predefined mathematical function employing M_1 and gk ,
14 calculating the value of M_2 ;

15 responsive to production of a value equivalent to r of the determining,
16 producing a message comprising M_1 and M_2 .

17
18 **23.** A medium as recited in claim 21, wherein the first predefined
19 mathematical function does not include the value of k , thus the value of k remains
20 unknown after the calculating the value of gk .

21
22 **24.** A medium as recited in claim 21, wherein the digital signature (*DS*)
23 has at least one other portion, *auth*, and the method further comprises:

24 determining whether a fourth predefined mathematical function employing
25 a secret key and gk produces a value equivalent to *auth*;

1 indicating the result of such determining.

2

3 25. A computing device comprising:

4 an audio/visual output;

5 a medium as recited in claim 21.

6

7 26. A method for facilitating digital security, the method comprising:

8 obtaining a message M having two portions, wherein M_1 is one of the
9 portions of the M and M_2 is another;

10 generating two or more codes having a combination with M_2 implicitly
11 embedded therein, wherein calculations that generate the codes do not employ M_2 ,
12 wherein the generating comprises:

13

- 14 • finding a value of a variable per-message key (k) where a predefined
15 mathematical function employing M_1 and g^k produces a result
16 equivalent to M_2 ;
- 17 • when such a value of k is found, calculating the two or more codes,
18 where the calculation of one code is not identical to the calculation
19 of any other code and where each calculation incorporates k ;

20 reporting the two or more codes.

21

22 27. A method as recited in claim 26 further comprising producing a

23 digital signature (DS) comprising M_1 and the reported two or more codes.

1 **28.** A digital signature (DS) produced by a method as recited in claim 27
2 and embodied on a computer-readable medium.

3
4 **29.** A digital signature (DS) produced by a method as recited in claim 27
5 and embodied as human-readable indicia on a human-readable medium.

6
7 **30.** A method as recited in claim 26, wherein the calculation of at least
8 one code employs a non-linear mathematical function.

9
10 **31.** A method as recited in claim 26, wherein the message M has a
11 defined length and a length of a combination of two or more codes is less than the
12 message's defined length.

13
14 **32.** A method as recited in claim 26, wherein M_2 has a defined length
15 and a length of a combination of two or more codes is less than or equal to the
16 defined length of M_2 .

17
18 **33.** A method as recited in claim 26, wherein one calculated code is r
19 and another is s , with r being calculated using another predefined mathematical
20 function employing M_1 and g^k , and with s being calculated using still another
21 predefined mathematical function employing M_1 and g^k and r .

22
23 **34.** A method as recited in claim 33, wherein the predefined
24 mathematical function for s is non-linear.

1 **35.** A method as recited in claim 33, wherein the predefined
2 mathematical function for s is quadratic.

3
4 **36.** A method as recited in claim 26 further comprising producing a
5 message comprising M_1 and the reported codes r and s .

6
7 **37.** A message produced by a method as recited in claim 36 and
8 embodied on a computer-readable medium.

9
10 **38.** A message produced by a method as recited in claim 36 and
11 embodied as human-readable indicia on a human-readable medium.

12
13 **39.** A method for facilitating digital security, the method comprising:
14 obtaining a digital signature (DS) having at least three portions, M_1 , r , and
15 s ;

16 using a first predefined mathematical function employing M_1 , r , and s ,
17 producing the value of gk ;

18 determining whether a second predefined mathematical function employing
19 M_1 and gk produces a value equivalent to r

20 indicating the result of such determining.

1 **40.** A method as recited in claim 39 further comprising:
2 using a third predefined mathematical function employing M_1 and gk ,
3 producing the value of M_2 ;
4 responding to production of a value equivalent to r of the determining,
5 producing a message comprising M_1 and M_2 .

6

7 **41.** A method as recited in claim 39, wherein the first predefined
8 mathematical function does not reference the value of k , thus the value of k remains
9 unknown after the calculating the value of gk .

10

11 **42.** A method as recited in claim 39, wherein the digital signature (DS)
12 has at least one other portion, *auth*, and the method further comprising:
13 determining whether a fourth predefined mathematical function employing
14 a secret key and gk produces a value equivalent to *auth*;
15 indicating the result of such determining.

16

17 **43.** A method as recited in claim 39, wherein the obtaining comprises
18 receiving input comprising the digital signature (DS) from a manual input unit of a
19 computing device.